National Infrastructure Protection Center

Password Protection 101

Every year thousands of computers are illegally accessed because of weak passwords. How many users are guilty of any of the following things:

- Writing down a password on a sticky note placed on or near your computer.
- Using a word found in a dictionary. That's right, a dictionary. Any dictionary!
- Using a word from a dictionary followed by 2 numbers.
- Using the names of people, places, pets, or other common items.
- Sharing your password with someone else.
- Using the same password for more than one account, and for an extended period of time.
- Using the default password provided by the vendor.

Chances are, if you are anything like the majority of computer users, you answered yes to one or more of the above questions. The problem is, hackers are aware of these problems as well and target those who don't take the correct precautions.

Why Is There A Problem?

Passwords are one of the first lines of defense that users have to protect their systems. Unfortunately, people are not accustomed to remembering difficult passwords consisting of numbers and weird characters. The ever-increasing number of passwords required to work in today's world only makes this problem worse. Many people have compensated for this problem by writing down their password and keeping that information in an unsecured area, like stuck to a computer screen.

One of the first things a hacker will attempt to do against a system is run a program that will attempt to guess the correct password of the target machine. These programs can contain entire dictionaries from several different languages. In addition to words found in dictionaries, these programs often contain words from popular culture such as science fiction movies and novels.

Hackers like to attack people's weaknesses. One of the major weaknesses is the reluctance to remember several, long, difficult to guess words such as passwords. Therefore, once one is chosen, the likelihood that the same password is used for several accounts is very high. This is similar to the problem with default passwords because users have a tendency to keep the same password for a long period of time, thereby allowing the attacker that much more time to gain access to a system.

What You Can Do?

Remembering long passwords can be difficult, but there are some basic techniques users can employ to lessen the pain. First, choose a phrase that you will remember. As an example, we will use the phrase "The pearl in the river." You can then take a number that you are familiar with, such as a birthday. For this example we will use 7/4/01. Next, you can take the first letter of your phrase and interlace it with the chosen date to make something similar to t7p4i0t1r. This method creates a password that won't be found in any dictionary and is unique to the person who created it.

t p i t r

=t7p4i0t1r

7 4 0 1

It is important to remember though, that any password can be guessed if given enough time. Therefore, it is important to change your password within the amount of time it would take an attacker to guess it. For example, with the previous password it may take an attacker 60 days on a very fast computer to guess what it is. In order to ensure your systems safety then, a user must change their password before those 60 days come to an end.

While password security is a very important deterrent to hackers gaining access to your system, it is only one component to the "defense in depth" principle. What this means, is a password need to be used along with other measures such as updated anti-virus software, firewall, etc.

Most Installation Policies:

1. **Passwords must be between 8 and 14 characters long.**

2. **Passwords must contain characters from *at least three* of the following *four* classes: upper case letters, lower case letters, numbers, special characters such as @, #, $, etc.**

3. **Passwords *may not* contain your user name or any part of your full name**